Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 15 August 2003

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The North American Electric Reliability Council reported that major losses of electric load occurred in the northeastern U.S. and Canada in the Eastern Interconnection Thursday. (See item 5)
- The Associated Press reports the Thursday blackouts in the eastern United States and parts of Canada seriously disrupted most modes of travel. (See item 13)
- The Department of Homeland Security has issued an advisory warning of "Potential Internet Attack Targeting Microsoft Beginning August 16, 2003." (See item 26)
- The CERT/CC has released an advisory warning that the system housing the primary FTP servers for the GNU software project, gnuftp.gnu.org, was root compromised by an intruder in March 2003. (See item 28)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *August 14, Reuters* — **Superconductor lines could boost U.S. power grids.** Scientists and power engineers say breakthroughs in superconductor research will bundle more electricity into ceramic−coated filaments less than the width of a human hair to deliver needed megawatts

through underground lines. **A U.S. Department of Energy program to reshape the nation's power grid −− "Grid 2030" −− says superconducting cables could relieve the congestion seen on many urban electric systems.** A superconductor is a material that is a perfect conductor of electricity when it is cooled to a super−cold minus 320 degrees Fahrenheit (minus 160 Celsius). Iced down by liquid nitrogen, a superconductor filament can carry three to five times more electricity than a conventional copper wire and without resistance. The power industry is working on early−stage projects for the new transmission wires in Long Island and Albany, NY, Columbus, OH, and other urban areas.
Source: http://www.forbes.com/business/energy/newswire/2003/08/14/rt r1057698.html

2. *August 14, The Associated Press* — **Boys detonated bombs at hydro plant.** According to local police, **three boys are accused of detonating homemade bombs at a Lancaster County, PA, hydroelectric plant.** Police said the teens mixed drain cleaner and aluminum foil in plastic soda bottles to make the explosion. **There was no report of damage** to the PPL Corp. plant in Marctic Township, PA.
Source: http://www.thewgalchannel.com/news/2405258/detail.html

3. *August 14, The Associated Press* — **Radioactive waste drum catches fire in Idaho. A radioactive waste drum being prepared for shipment to New Mexico caught fire at the Idaho National Engineering and Environmental Laboratory.** A laboratory spokesperson said that lab workers noticed that the drum was bulging with gases, which is common and is usually solved by venting the drum. However, this time there were flames. No one was injured. The drum contains radioactive waste from the Rocky Flats nuclear weapons plant in Colorado. The waste was being prepared for shipment to the Waste Isolation Pilot Plant near Carlsbad.
Source: http://kobtv.com/index.cfm?viewer=storyviewer&id=3704&cat=HO ME

4. *August 14, Government Accounting Office* — **Report−GAO−03−426: Spent Nuclear Fuel: Options Exist to Further Enhance Security.** Spent nuclear fuel, the used fuel periodically removed from nuclear power reactors, is one of the most hazardous materials made by man. Nuclear power companies currently store 50,000 tons of spent fuel at 72 sites in 33 states. That amount will increase through 2010, when the Department of Energy (DOE) expects to open a permanent repository for this fuel at Yucca Mountain, NV. Concerns have been raised since September 11, 2001, that terrorists might target spent fuel. **GAO was asked to (1) review federally sponsored studies that assessed the potential health effects of a terrorist attack or a severe accident on spent fuel, either in transit or in storage, and (2) identify options for DOE to further enhance the security of spent fuel during shipping to Yucca Mountain.** GAO recommended that, as DOE develops its plans for transporting spent fuel to Yucca Mountain, it assess potential options to further enhance the security and safety of this fuel.
Source: http://www.gao.gov/highlights/d03426high.pdf

5. *August 14, North American Electric Reliability Council* — **NERC Announcement: Power Outages Affect Northeast and Canada.** Starting at about 4:11 PM EDT on Thursday, August 14, major losses of electric load occurred in the northeastern U.S. and Canada. **Although the exact cause is not known at present, the outages are not the result of a physical or cyber terrorist attack**. The areas most affected center around the Great Lakes: Michigan, Ohio, New York City, Ontario, Quebec, northern New Jersey, Massachusetts, and Connecticut. **The disturbance appears to have largely been caused by the loss of several major transmission**

lines in the upper Midwestern United States, which caused additional lines to go out of service as well as major fossil and nuclear power plants. A large number of nuclear plants in the affected areas went off−line and may take several days to return to service. Most fossil−fired generation has been restored to service. Although the event was felt throughout the entire Eastern Interconnection, customers and utilities in the south and western part of the Interconnection were not affected.
Source: http://www.nerc.com/8−14−03−outage−announcement3.pdf

6. *August 13, North American Electric Reliability Council* — **NERC board votes to adopt cyber security standard. The Board of Trustees of the North American Electric Reliability Council (NERC) has voted to adopt a cyber security standard that will reduce risks to the reliability of the bulk electric system from any compromise of critical cyber assets,** including computers, software, and the communication networks that support those systems. The standard requires that critical cyber assets related to the reliable operation of the bulk electric systems are identified and protected. The standard and its associated implementation plan are effective for one year from the date of adoption. The board's action follows an industry action to approve the standard by a weighted vote of 72.6 percent. The board's approval means that this is the first standard to go through NERC's new, ANSI−accredited process for developing reliability standards.
Source:
ftp://www.nerc.com/pub/sys/all_updl/docs/pressrel/8−13−03−Cyber−Standard−Board−PR.pdf

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

7. *August 14, The Courier−Journal (KY)* — **Navy unveils new defense system. The SeaRAM system is designed to defend U.S. ships against any enemy, including terrorists, on both sea and shore.** The SeaRAM combines and upgrades elements of two Navy weapons systems. It uses sensors of a Phalanx Gatling gun system and elements of a RAM (rolling airframe missile) system that can fire 11 guided missiles in rapid order. The Navy expects in a few years to have the SeaRAM operative on up to 200 ships. **The system is designed to greatly increase the distance that enemy weapons can be detected,** however, it might be as long as 18 months before the SeaRAM system is ready for deployment aboard ships. The SeaRAM's detection system is designed to track helicopters, small boats or land−based weapons, and its imaging−detection system operates day or night.
Source: http://www.courier−journal.com/business/news2003/08/14/biz−front−rayth14−5642.html

8. *August 14, American Forces Press Service* — **Anti−terror war drives DoD transformation efforts.** The ongoing war against global terrorism makes U.S. military transformation efforts an

imperative goal, according to Air Force General Richard B. Myers, the chairman of the Joint Chiefs of Staff, Defense Secretary Donald H. Rumsfeld. **At a meeting on Thursday, August 14, Rumsfeld said that the DoD must continue its transformation to meet 21st century threats, such as terrorism. This requires U.S. military forces to become "lighter, more agile," the secretary pointed out, as well as overhauling the way the department administers its civilian workforce,** such as by using performance as a metric for rewards rather than seniority. The fruits of DoD transformation efforts are evident even today, the secretary pointed out, noting that the recent conflicts in Afghanistan and Iraq required "far fewer troops" and less time to assemble forces and materiel than in past wars.
Source: http://www.defenselink.mil/news/Aug2003/n08142003_200308144. html

[Return to top]

Banking and Finance Sector

9. *August 14, Reuters* — **Blaster worm claims Nordea bank. The "Blaster" Internet worm infected servers in all of Nordea's 440 Finnish bank offices, forcing the one−day closure of about 80 branches on Thursday, August 14.** Nordea has assigned a technical team to flush the infection out of its computers overnight. A Nordea spokesperson said that the worm had not affected its Internet banking system or corrupted any customer data.
Source: http://www.finextra.com/fullstory.asp?id=9744

10. *August 14, Reuters* — **Wall Street turns on emergency power after outage.** Wall Street turned on emergency power and stock trading was sharply reduced after−hours on Thursday, August 14, 2003, after massive power outages hit New York, other cities in the northeastern United States and parts of Canada. **The New York Stock Exchange and Nasdaq are set to open on Friday morning as usual, and most major Wall Street firms said contingency plans were working well and emergency power generators were running smoothly.** U.S. power regulators said the massive power outage was not caused by a terror attack, but traders said Wall Street was still a bit edgy. One trader said that among the biggest problems Wall Street was facing was processing trades overnight for options set to expire Friday morning. "I would imagine there would have to be some provision to make sure that people who made closing transactions in the morning don't in fact get exercised in the morning," said Rob Coggan, a trader. "It's a bookkeeping problem." If power is restored by the time U.S. stock markets are scheduled to open at 9:30 a.m., there will likely be little impact on the financial markets, traders said. **The U.S. Securities and Exchange Commission said it was carefully monitoring the power failure and was in regular communication with the markets and clearing agencies**.
Source: http://biz.yahoo.com/rf/030814/markets_stocks_power_4.html

[Return to top]

Transportation Sector

11. *August 14, New York Times* — **Air industry backs a bill to privatize control jobs. Airport and airline officials today gave strong support to a bill that would allow the Federal**

Aviation Administration to contract out the jobs of more than 2,000 controllers, saying the move would save money without harming safety. The bill, which would authorize $60 billion in spending by the aviation administration over the next four years, also provides money needed for war risk insurance, security improvements and air traffic control modernizations, according to James C. May, the president and chief executive of the Air Transport Association, the airline trade group. **The new bill, now in the form of a conference report reconciling differing House and Senate versions, would permit the aviation agency to contract out about 2,000 jobs of controllers who work in Flight Service Stations, offices that do not direct traffic, but provide briefings, mostly to private pilots, on weather and temporary airspace restrictions.** It would also let the agency contract out hundreds of other jobs at 69 air traffic towers, mostly at smaller airports but at some large ones.
Source: http://www.nytimes.com/2003/08/14/politics/14PRIV.html

12. *August 14, CNN* — **Pentagon willing to share airline defense technology. The Pentagon on Thursday said the Defense Department would make available to commercial airlines the technology used by military jets to protect against shoulder−fired, surface−to−air missiles −− if the industry requested it.** "My guess is, if they wanted the technology we have on some of our military aircraft to defeat this threat, it would be made available. It's a widely available technology, though fairly sophisticated," Chairman of the Joint Chiefs of Staff Gen. Richard Myers said at a town hall meeting at the Pentagon. The threat that those missiles could down a civilian plane has existed for several decades, Myers said, and noted that 35 to 40 such attempts have been made with some success. **The Department of Homeland Security has asked eight government contractors to devise plans for anti−missile technology that could be put on commercial airliners. Since September 11, 2001, advisories have been sent to air carriers citing the possible threat to commercial aircraft from shoulder−fired missiles.** One sent in May discussed intelligence indicating al Qaeda had an interest in using missiles against commercial aviation in North Africa and the Middle East.
Source: http://www.cnn.com/2003/US/08/14/jets.missiles/index.html

13. *August 14, The Associated Press* — **Transportation affected by blackout.** The blackouts in the eastern United States and parts of Canada disrupted travel by planes, trains, and automobiles. **Flights in and out of Kennedy and LaGuardia airports in New York, as well as airports in Newark, NJ, Cleveland, OH, Toronto and Ottawa were grounded for several hours** because there was no power to run the metal detectors and X−ray machines at security screening checkpoints, Transportation Department spokesman Leonardo Alcivar said. Difficulties also developed at other airports: Northwest Airlines curbed flights into Detroit, and US Airways reported problems in Albany and Rochester, NY, Erie, PA, and Montreal. Ground transportation didn't fare much better. **Amtrak halted travel between New Haven, CN, and Newark, NJ, including New York's Pennsylvania Station. New York subways stopped in their tracks, forcing evacuations of passengers, and bridges and tunnels were closed to inbound traffic** −− albeit open for motorists leaving Manhattan.
Source: http://www.newsday.com/news/local/newyork/ny−bztransport0814,0,7241446.story?coll=ny−top−headlines

[Return to top]

Postal and Shipping Sector

14. *August 14, DM News* — **Bill would limit Post Office closures.** Senator Harry Reid has proposed a law that would curb the U.S. Postal Service's (USPS) ability to close post offices in rural areas and allot federal grants to mitigate economic effects when it does make a closure. **The bill would require the USPS to prove that closing post offices in areas with populations of less than 20,000 would have a positive effect on the economy and quality of life in the area.** The USPS would have to presume that the closure would have a negative effect unless it proved otherwise. If the USPS determined that a post office in a rural community should be closed, it would have to develop a plan to rehabilitate the building according to the wishes of the people of the community, according to the proposal. **In its recommendations unveiled last month, the postal reform commission appointed by the president argued that the USPS should be granted greater authority to close post offices when they are unprofitable.**
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=2476 3

[Return to top]

Agriculture Sector

15. *August 14, Associated Press* — **Cattle quarantined. About 160 cattle are quarantined on a ranch north of Newell, SD, where 16 cattle have died of anthrax in the last week**. State veterinarian Sam Holland says the deaths mark South Dakota's first case of the disease in livestock this year. He says the animals were not vaccinated and he would not release the name of the rancher who owns the land. **The cattle likely got the anthrax because dry weather the past two summers has kept grass short.** That forces the cattle to eat closer to the ground and come in contact with more soil. The Butte County ranch where the anthrax was found is about 30 miles from seven ranches that had confirmed cases last year.
Source: http://www.ksfy.com/Global/story.asp?S=1400446&nav=0w0jHRWF

16. *August 14, Guardian* — **Scientists to check whether deer can get BSE. Scientists are planning to feed and inject deer with bovine spongiform encephalitis (BSE) infected tissue to see whether they can contract the disease**. The lab tests are being organized as concern mounts about the spread in deer and elk in the U.S. of a similar disease to BSE called chronic wasting disease (CWD). Carcasses and brains of wild and farmed deer are soon likely to be tested for BSE, CWD, or scrapie, a disease endemic in British sheep but never linked to human fatalities. One of the theories for BSE suggests scrapie jumped to cattle and became a far more virulent danger to people consuming their meat. Government officials say no BSE−like disease has been reported in European deer under natural conditions. The U.S. is further advanced in experimenting to find out whether its deer disease could spread to cattle. **Injections of CWD into the brains of cattle have produced signs of damaged prions, the proteins thought responsible for such diseases. But feeding CWD material to cattle has so far failed to infect them.**
Source: http://www.guardian.co.uk/uk_news/story/0,3604,1018298,00.ht ml

17. *August 14, Associated Press* — **More deer and elk quarantined. Wisconsin has quarantined five captive deer and elk herds that may have been exposed to chronic wasting disease** (CWD). The animals may have been exposed to the deadly brain disease through contact with

infected wild deer, acting state veterinarian Dr. Robert Ehlenfeldt said Wednesday. The herds live within the boundaries of the Department of Natural Resources' (DNR) CWD eradication zone around Mount Horeb. **The captive herds have shown no sign of the disease, but the state placed them under quarantine because they live within the expanded zone**, according to the Department of Agriculture, Trade and Consumer Protection. The DNR wants to kill as many deer as possible in the zone to keep the disease from spreading. The quarantine means no live deer or elk can move off the farms except to go directly to slaughter. Any slaughtered animals must be tested for CWD. No live test for the disease exists.
Source: http://www.wisinfo.com/postcrescent/news/archive/local_11746 404.shtml

[Return to top]

Food Sector

18. *August 14, Associated Press* — **Monitoring the chemicals we eat.** Four times a year, Food and Drug Administration (FDA) employees enter grocery stores in three different cities with identical lists. They ship purchases to an FDA laboratory in Kansas, where workers sort the food, sending ingredients that need cooking on to a kitchen in Missouri. Inside the lab, scientists then test for more than 300 pesticides, cancer−causing dioxins, and industrial chemicals. The Total Diet Study measures traces of chemicals in the average diet both in packaged foods and after consumers wash produce, mix up ingredients, and properly cook a meal. **This monitoring enables health officials to spot whether changes in food production or the environment affect food quality. In response, they can launch medical research, alter regulations, or if a problem is bad enough, recall a brand.**
Source: http://www.enn.com/news/2003−08−14/s_7456.asp

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

19. *August 14, Miami Herald* — **Malpractice overhaul.** The Florida legislature on Wednesday passed a plan to overhaul the state's medical malpractice insurance system. **The bill will cap the pain and suffering amount that juries can award a victim of medical malpractice at $1.25 million in most cases, with physicians' liability capped at $500,000 and hospitals' or other medical providers' liability capped at $750,000.** For cases resulting in death or other serious injuries, such as blindness or loss of reproductive ability, the cap can grow to $2.5 million, $1 million from doctors and $1.5 million from medical facilities. The bill, which takes effect September 15, will freeze doctors' insurance rates through the end of the year and could mandate a rate rollback come January. But the size of that rollback, if any, will be unknown until state regulators estimate the cost savings from the changes to the insurance system. Insurance companies will be allowed to challenge the findings.

Source: http://www.miami.com/mld/miamiherald/6527598.htm

20. *August 14, Boulder Daily Camera* — **West Nile case count up. Boulder County, Colorado had its largest one−day total of confirmed West Nile cases Wednesday as 10 more people tested positive for the mosquito−borne virus.** The county now has 38 reported cases of West Nile, including three infections that have developed into meningitis, a potentially fatal inflammation the lining of the brain and spinal cord. State health officials said Wednesday that **32 new cases were confirmed statewide, bringing Colorado's total for the summer to 247.** Six people in Colorado have died of complications from the virus. Three−quarters of Colorado's human carriers suffer from West Nile fever, a more benign complication of the virus than meningitis or encephalitis. Symptoms of the fever include headache, fever, nausea and a rash.
Source: http://www.bouldernews.com/bdc/county_news/article/0,1713,BDC_2423_2181641,00.html

21. *August 13, Associated Press* — **Canada reports second SARS death in three days. A health−care worker died of Severe Acute Respiratory Syndrome (SARS) on Wednesday, becoming the 44th person killed by the pneumonia−like illness in Toronto, Canada, and the second to die this week.** The latest deaths come nearly six weeks after the World Health Organization removed Toronto from its list of SARS−infected areas, saying the city had contained the outbreak. **Eight people remain hospitalized with SARS in Toronto**, where almost 250 cases were recorded in two outbreaks earlier this year. The latest SARS victim was identified by Ontario health officials as a 54−year−old male health care worker. On Monday, a 44−year−old patient died of SARS in Toronto.
Source: http://www.guardian.co.uk/worldlatest/story/0,1280,−3024086, 00.html

[Return to top]

Government Sector

22. *August 14, Federal Computer Week* — **Border agency tests monitors.** The Bureau of Customs and Border Protection will embark on a pilot project to automate the monitoring of intrusions along the border. **Analyzing border videos and sensors to present a single, real−time image of the region, the Security Data Management System software recognizes events from streams of data and maps the events for a single agent to monitor. The initial test covers one sector along the U.S. border with Mexico.** Border officials can use the Secure Data Management System to set policies, such as which objects can cross a certain part of the border at a certain time. The software then takes the unstructured data from video streams and pulls out structured data, such as the size, time and location of an object on the border. That information is plotted on a three−dimensional display at a console, allowing a single agent to monitor the area.
Source: http://www.fcw.com/fcw/articles/2003/0811/web−cust−08−13−03. asp

[Return to top]

Emergency Services Sector

23. *August 15, CNN* — **Major power outage brings emergency efforts.** The cause of a blackout that affected all of New York City and much of the Northeast on a sweltering August day remained uncertain Friday morning as power began to trickle back to a few, even as more than 15 million from Detroit to Ottawa remained without electricity. Rob Glenn with the Ohio Emergency Agency said **50 National Guard troops have been deployed with 450−gallon tank trucks to distribute water to areas of greater Cleveland that are having problems after electric water pumps shut down**. Early Friday, New York City Mayor Michael Bloomberg said he hopes most of New York City will have power restored in time for Friday's morning rush hour. Police and volunteers were on street corners throughout New York City directing traffic because all the stoplights were out. Bloomberg said **40,000 police officers and the entire fire department were being deployed during the night to maintain calm in New York. Pataki said "well over half" of the state's population was affected by the blackout, and he declared a statewide state of emergency**.
Source: http://www.cnn.com/2003/US/08/15/power.outage/index.html

24. *August 14, National Institute of Standards and Technology* — **Finding dirty bombs and other radiation threats.** In an age of terrorism, law enforcement agents and other first responders need to be prepared for a wide range of threats, including so−called "dirty bombs" and other radiation hazards. To help ensure the performance of devices used to detect such threats, **National Institute of Standards and Technology (NIST) researchers are working with the Institute of Electrical and Electronics Engineers (IEEE) and the American National Standards Institute (ANSI) to develop new standards for a variety of radiation detectors and monitors.** With partial funding from the Department of Homeland Security (DHS) and NIST's Office of Law Enforcement Standards, NIST researchers are investigating a wide variety of detection devices, ranging from 3−meter−high portal towers that scan truck trailers while they move through checkpoints to small, pager−size monitors that serve as personal dosimeters. **The new standards under development will ensure that the devices work as intended under the new conditions now encountered in homeland security related tasks.** The accuracy rates for 19 different hand−held detectors ranged within plus or minus 5 percent of the actual radiation value to plus or minus 40 percent depending on whether they were measuring high, medium or low energy radiation sources.
Source: http://www.sciencedaily.com/releases/2003/08/030814072428.ht m

25. *August 14, Chicago Sun Times* — **City seeks federal money to buy high−rise rescue equipment. Equipment for high−rise rescues is expected to make Chicago's wish list for the $10.8 million in federal money being made available to the city to respond better to terrorist attacks and other emergencies**, officials said Wednesday. On July 30, the U.S. Department of Homeland Security announced the city was eligible for the Urban Security Initiative funds. Chicago's wish list has not been finalized, but a Fire Department official said the city needs new equipment to respond to emergencies like one this week in which sewer workers were pulled from a collapsed trench. **The city also wants new "high−angle" rescue equipment for scaffold collapses and other skyscraper disasters; a "light wagon" to illuminate nighttime disaster sites; a hazardous materials rig, and more protective gear, the official said.** The Fire Department might ask for a high−tech boat to patrol the lakefront and augment an existing vessel. But such a boat, which would cost about $1 million, is not likely to win federal approval, a source said.
Source: http://www.suntimes.com/output/terror/cst−nws−terror14.html

[Return to top]

Information and Telecommunications Sector

26. *August 14, U.S. Department of Homeland Security* — **Potential Internet Attack Targeting Microsoft Beginning August 16, 2003.** An Internet worm dubbed "msblast", "lovesan", or "blaster" that began spreading on Monday takes advantage of a recently announced vulnerability in computers running some versions of the Microsoft Windows operating system. **This worm contains additional code which may cause infected computers to attempt repetitive connections to a Microsoft web site, www.windowsupdate.com, beginning Saturday, August 16, which may result in a distributed denial of service (DDoS) attack**. DHS encourages system administrators and computer owners to update vulnerable versions of Microsoft Windows operating systems as soon as possible before August 15th. System administrators and computer owners should also update anti−virus software. Details on which computers are vulnerable and instructions for cleaning infected computers are available at: http://www.microsoft.com/security/incident/blast.asp.
Source: http://www.dhs.gov/interweb/assetlibrary/Advisory_Internet_A ttack_081603.PDF

27. *August 14, Federal Computer Week* — **DHS rushes to finish tech plan.** By week's end, the Department of Homeland Security (DHS) wants to finish the document that will define the future of the agency's information technology and business structure. **The DHS has a Friday deadline for the initial draft of its enterprise architecture**. It will be for internal review only, said Lee Holcomb, chief technology officer at DHS. The transition strategy−−outlining how officials expect to combine the existing jumble of systems across the 22 organizations into a coherent and consolidated tech infrastructure−−is due by October. Holcomb spoke Wednesday at a conference on solutions architects.
Source: http://fcw.com/fcw/articles/2003/0811/web−dhs−08−14−03.asp

28. *August 13, CERT/CC* — **CERT Advisory CA−2003−21 GNU Project FTP Server Compromise . The system housing the primary FTP servers for the GNU software project, gnuftp.gnu.org, was root compromised by an intruder in March 2003**. The more common host names of ftp.gnu.org and alpha.gnu.org are aliases for the same compromised system. The potential exists for an intruder to have inserted back doors, Trojan horses, or other malicious code into the source code distributions of software housed on the compromised system. Because this system serves as a centralized archive of popular software, the insertion of malicious code into the distributed software is a serious threat. However, no source code distributions are believed to have been maliciously modified at this time. **The CERT/CC encourages sites using the GNU software obtained from the compromised system to verify the integrity of their distribution**. The original FSF advisory is available here: ftp://ftp.gnu.org/MISSING−FILES.README.
Source: http://www.cert.org/advisories/CA−2003−21.html

Current Alert Levels

 AlertCon: 3 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 3 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.F** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 80 (www), 137 (netbios−ns), 1434 (ms−sql−m), 113 (ident), 0 (−−−), 53 (domain), 139 (netbios−ssn), 25 (smtp) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

29. *August 14, Reuters* — **Australia warns of Indonesia attacks. Australia and New Zealand have received information that terror attacks could be launched against Indonesia on Sunday, August 17, Indonesia's national day.** New Zealand's ambassador to the southeast Asian country has written to up to 900 New Zealand citizens registered with their Jakarta embassy warning of reports that "terrorist groups are planning attacks." **The Indonesian government planned tighter security at possible targets and in public places, including a bigger police presence.** The U.S. embassy in Jakarta had advised its nationals on Wednesday "to take special precautions regarding their personal security and avoid large gatherings" on the weekend.
Source: http://www.msnbc.com/news/949362.asp?0sl=−21&cp1=1

30. *August 14, New York Times* — **Pirates attack ships in Malacca Strait and hold three for ransom.** Heavily armed pirates have attacked two ships in the Strait of Malacca in the last week and are still holding the captain, chief engineer and an assistant engineer from one of the vessels as hostages. **Both incidents appear to involve pirates operating from bases on the Indonesian side of the strait. The International Maritime Bureau regional piracy center in Kuala Lumpur, Malaysia, has urged vessels passing through the strait to stay close to the Malaysian side of the waterway**. With half the world's oil shipments by sea passing from the Persian Gulf through the Strait of Malacca to east Asia, the strait trails only the Strait of Hormuz at the mouth of the gulf as an oil shipping lane. Pirates have stolen six tugboats so far this year so Singapore restricted the movements of tugboats in its waters earlier this year because of fears that terrorists would use them to mount an attack.
Source: http://www.nytimes.com/2003/08/14/international/asia/14CND−P IRA.html

31. *August 14, Associated Press* — **Key al Qaeda figure captured. The White House announced**

Thursday, August 14, the capture of a man described as al Qaeda's chief representative and operational planner in Southeast Asia, calling his apprehension "a significant blow to the enemy." He was identified as Riduan Isamuddin−−also known as Hambali. A senior administration official described the suspect as "one of the world's most lethal terrorists" and said his group, Jemaah Islamiya, was linked to last year's Bali bombing and a series of deadly church bombings in the Philippines. **He is also a leading suspect in the JW Marriot bombing in Jakarta and a close associate of Khalid Shaikh Mohammed, the alleged September 11 mastermind** who was captured earlier this year. Hambali was captured in southeast Asia and is now in U.S. custody at an undisclosed location, officials said. Hambali is also connected the the September 11 plot, although it's unclear how much of a direct role he played. Authorities say Hambali ordered one of his deputies to host meetings between two eventual September 11 hijackers, Khalid al−Mihdhar and Nawaf al−Hazmi, and another high−ranking al Qaeda figure, at his apartment in Malaysia in January 2000.
Source: http://www.washingtonpost.com/wp−dyn/articles/A58761−2003Aug 14.html

32. *August 13, U.S. Department of State* — **Travel Warning: Saudi Arabia. The Department of State warns U.S. citizens to defer non−essential travel to Saudi Arabia**. Americans are reminded of the potential for further terrorist actions against U.S. citizens abroad, including in the Persian Gulf region. **The U.S. Government has received indications of terrorist threats aimed at American and Western interests, including the targeting of transportation and civil aviation**. American citizens in Saudi Arabia should remain vigilant, particularly in public places such as residential areas, clubs, restaurants, places of worship, hotels, schools, airports, outdoor recreation events, resorts and beaches, etc. U.S. citizens who travel to, or remain in, Saudi Arabia should register at the Consular Section of the U.S. Embassy in Riyadh or at the Consulates in Jeddah and Dhahran and enroll in the warden system (emergency alert network) in order to obtain updated information on travel and security in Saudi Arabia.
Source: http://travel.state.gov/saudi_warning.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer